

```

START ADDRESS?F5E0
F5E0: A0 FF 02 LDA $02FF
F5E3: 00 FB BNE $F5E0
F5E5: A2 02 LDX #$02
F5E7: B5 54 LDA $54,X
F5E9: 95 5A STA $5A,X
F5EB: CA DEX
F5EC: 10 F9 BPL $F5E7
F5EE: A0 FB 02 LDA $02FB
F5F1: A8 TAY
F5F2: 2A ROL A
F5F3: 2A ROL A
F5F4: 2A ROL A
F5F5: 2A ROL A
F5F6: 29 03 AND #$03
F5F8: AA TAX
F5F9: 98 TYA
F5FA: 29 9F AND #$9F
F5FC: 1D F6 FE ORA $FEF6,X
F5FF: 8D FA 02 STA $02FA
F602: 20 47 F9 JSR $F947

```

6502 DISASSEMBLER

A Disassembler and
ASCII Converter
For The ATARI 400/800

Written in BASIC
By Bob Pierce

A
product
of



QUALITY SOFTWARE

LOADING INSTRUCTIONS

6502 DISASSEMBLER is a BASIC program and is written to run on any ATARI 400 or ATARI 800 computer. The program requires only 8K of memory to operate. To load the tape, follow these steps:

1. Be sure that the BASIC cartridge is in your ATARI computer. Turn on your computer and place the tape in the ATARI 410 program recorder. Rewind the tape.
2. Press the PLAY switch on the recorder. After the computer has displayed the READY message, type CLOAD and press the RETURN key. You will hear a short buzz. Then press the RETURN key again and the tape recorder will begin to run. After about two minutes, the program will finish loading, the computer will display a READY message, and you will be able to run the program.

Should you be unable to load the tape after several attempts, there is a second copy of the program on the tape following the first.

STARTING

To run the 6502 DISASSEMBLER, type RUN and press the RETURN key. This will also start the program again after you have stopped it by pressing the BREAK key.

The program will display the question

PRINTER(Y/N)?

Type Y and press the RETURN key if you wish the output to go to your printer. Pressing any other key followed by the RETURN key will cause the output to go to the video. The computer will respond with the question:

ASCII(A) OR INSTRUCTIONS(I)?

If you wish to disassemble a machine language program such as the ATARI BASIC or the ATARI Monitor, type I and press the RETURN key. If you wish to inspect an area of a program for the presence of ASCII code, type A and press RETURN.

The default values for these two questions are N and I. If you simply press RETURN in response to each of these questions, the program will not send the output to the printer and will disassemble machine code instructions.

The next question displayed will be:

START ADR?

Type in the address in hexadecimal at which you wish disassembly or ASCII conversion to begin. The ATARI Monitor begins at the hexadecimal address D800. Some important ASCII in ATARI BASIC begins at A4B1. After a hexadecimal address of between one and four digits has been typed, press RETURN and the program will commence listing the output.

If you have only 8K of user memory, then disassembling a user program of any size is not practical because the 6502 DISASSEMBLER program uses all available user memory. When you expand beyond 8K, however, just about any program can be disassembled by storing it at an address greater than 2000H. The monitor and the BASIC cartridge can be disassembled on any size ATARI computer.

STOPPING AND RESTARTING

To halt the disassembly temporarily, hold down the CTRL key and press the 1 key. The halted assembly can be resumed by pressing CTRL-1 again. To stop the disassembly, press the BREAK key.

If you stop the disassembly with the BREAK key, and then wish to restart it from where it stopped, you may do so by typing CONT and pressing RETURN. This will sometimes cause an error because the CONT command begins execution at the line number following the line number in which the BREAK occurs.

To start a new disassembly without clearing the screen type GO 100 and press RETURN. To clear the screen and start a new disassembly type RUN and press RETURN.

OUTPUT

on the cover of this booklet is an example of a disassembly of instructions in the ATARI monitor. Listed below is another example.

```
D800: 20 A1 DB JSR $DBA1
D803: 20 BB DB JSR $DBBB
D806: B0 39 BCS $D841
D808: A2 ED LDX #$ED
D80A: A0 04 LDY #$04
```

The data on each line of output consist of the following fields:

HEXADECIMAL ADDRESS. The first four digits listed on a line to the left of the colon represent the hexadecimal address of the instruction.

MACHINE CODE INSTRUCTION. The next field of data is a one to three byte machine language instruction code. Each byte is represented by two hexadecimal digits. Based on the first byte of the instruction, the 6502 DISASSEMBLER program calculates the length of the instruction and places the appropriate number of bytes in this field.

6502 ASSEMBLY LANGUAGE INSTRUCTION. The last field of each output line contains the assembly language instruction. The "branch" instructions (BCS, etc.) contain the calculated absolute address. Although the program will process code from tables and ASCII messages as if it were instructions, it is usually easy to detect when this happens.

In the ASCII mode (obtained by selecting 'A'), the 6502 ASSEMBLER lists the ASCII representation of the code found in memory. For example:

```
A4B0: ?RE???DAT???INPU
A4C0: ???COLO?2?LIS?#?
```

The ASCII representation of 16 bytes of code are listed on each line, preceded by the address of the first byte. Wherever a "?" appears, it means that there is no ASCII conversion value for that particular byte. This is the case when the byte has a hexadecimal value of less than 20H or greater than 7AH.

6502 DISASSEMBLER FOR THE ATARI 400/800

6502 DISASSEMBLER is a program written in ATARI BASIC. It performs two functions:

1. It is a disassembler
2. It is an ASCII dumper

Both of these functions require a program, and both are very useful, and oftentimes desperately needed, especially by the assembly language programmer.

What is a disassembler? It is a program that does the exact reverse of an assembler. It runs through memory, takes the machine code instructions that are there, and converts them back to the assembly language instructions which they represent.

With the 6502 DISASSEMBLER program an assembly language listing can be obtained of the ATARI Monitor or ATARI BASIC or machine language programs in RAM. The output always appears on the video and may be sent to an ATARI printer or any printer that recognizes the LPRINT statement. The program also converts code in memory to ASCII if possible, and dumps the results to the video or printer.



QUALITY SOFTWARE

6660 Reseda Blvd., Suite 105, Reseda, CA 91335

(213) 344-6599

LOADING INSTRUCTIONS

6502 DISASSEMBLER DISKETTE

The 6502 DISASSEMBLER diskette does not have a copy of DOS on it. Using one of your own diskettes, boot DOS with the BASIC cartridge inserted. You must also have at least 24K of RAM in your Atari 800.

Insert the 6502 DISASSEMBLER diskette into disk drive number 1. Run the program by typing the BASIC command:

RUN "D:DISASM"

The program should load and execute, clearing the screen and displaying a copyright statement and the question, "PRINTER(Y/N)?". See the accompanying booklet for further instructions.